Security Advisory 2023-026

Critical Vulnerability in a Cisco Product

May 5, 2023 — v1.0

TLP:CLEAR

History:

- *05/05/2023 — v1.0 – Initial publication*

Summary

On May 3, 2023, Cisco released an advisory to address a critical vulnerability in the web-based management system of the Cisco SPA112 2-Port Phone Adapters. The vulnerability is tracked as `CVE-2023-20126` and has a CVSS score of 9.8 [1].

Technical Details

A vulnerability in the web-based management interface of Cisco SPA112 2-Port Phone Adapters could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. This vulnerability is due to a missing authentication process within the firmware upgrade function. An attacker could exploit this vulnerability by upgrading an affected device to a crafted version of firmware. A successful exploit could allow the attacker to execute arbitrary code on the affected device with full privileges [1].

There are currently no reports yet of an active exploitation of this vulnerability [2].

Affected Products

This vulnerability affects all firmware releases for Cisco SPA112 2-Port Phone Adapters [1].

Moreover, Cisco has not released and will not release firmware updates to address the vulnerability, because Cisco SPA112 2-Port Phone Adapters have entered the end of-life process and are no longer supported [1].

Recommendations

CERT-EU encourage constituents to discontinue using the product, as well as verify if any other similar – possibly also no longer supported – products are in use.

Workarounds

There are no workarounds that address this vulnerability.

References

[1] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-unauth-upgrade-UqhyTWW

[2] https://www.bleepingcomputer.com/news/security/cisco-phone-adapters-vulnerable-to-rce-attacks-no-fix-available/